

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA,

v.

ROGER J. STONE, JR.,

Defendant.

Criminal No. 19-cr-18-ABJ

**DEMOCRATIC NATIONAL COMMITTEE AND DCCC'S MEMORANDUM IN
SUPPORT OF THEIR MOTION FOR LEAVE AND OPPOSITION TO DEFENDANT'S
REQUEST FOR RULE 17(C) SUBPOENA**

The Democratic National Committee ("DNC") and DCCC, a/k/a Democratic Congressional Campaign Committee, hereby submit this Memorandum in Support of their Motion for Leave and Opposition to Defendant Roger Stone's "*Motion for an Order Permitting Defendant Roger J. Stone to Issue Early Return Subpoena Duces Tecum to CrowdStrike Holdings, Inc., CrowdStrike Services, Inc., and CrowdStrike, Inc., Pursuant to Federal Rule of Criminal Procedure 17(c)*" (hereinafter, "Motion to Subpoena CrowdStrike" or "subpoena request"), ECF 160.

INTRODUCTION

Defendant Roger Stone has asked this Court to grant him unfettered access to privileged and highly sensitive documents that would reveal internal strategies of his political opponents, but are entirely irrelevant to the charges levied against him. Specifically, Stone's request for a Rule 17(c) subpoena seeks unredacted versions of three reports that were prepared by CrowdStrike¹ at the instruction of counsel for the DNC and DCCC, for the purpose of providing legal advice on the heels of an unprecedented cyberattack orchestrated by Russian-based hackers during the 2016 presidential election. While Stone's request is directed toward CrowdStrike, the documents he

¹ Defendant's requested subpoenas are addressed to CrowdStrike Holdings, Inc., CrowdStrike Services, Inc., and CrowdStrike, Inc. This Motion will refer to the three entities collectively as "CrowdStrike."

seeks—and the privileges they implicate—belong to the DNC and DCCC, which are the proper targets of his subpoena. Both organizations (among other high-profile Democrats) were victims of the 2016 cyberattack and have a strong interest in preventing the publication of the unredacted reports that contain, among other things, recommendations for remediating and preventing future attacks, which are protected by the attorney-client privilege, the work product doctrine, and the First Amendment privilege, and the release of which would potentially expose the DNC and DCCC to significant harm.

The information Stone seeks, to be sure, has no evidentiary value in this case. The grand jury's seven-count indictment charges Stone with obstructing investigations into Russian interference in the 2016 presidential elections, lying to Congress, and witness tampering, none of which have anything to do with CrowdStrike's investigation of the DNC and DCCC cyberattack. It is telling that Stone's Motion makes no reference to any of the false statements that he is accused of making, and instead relies entirely on wishful thinking that he might uncover evidence showing that Russian intelligence was not involved in the DNC and DCCC cyberattack, notwithstanding the consensus of the U.S. intelligence community.²

But even if Stone were to find such evidence, CrowdStrike's investigation could not possibly be relevant to any plausible defense against the perjury and witness tampering allegations set forth in the indictment. Although the Government does not intend to respond to Stone's subpoena request, it, too, has made clear in previous filings that the unredacted reports are not relevant to the charges against Stone. ECF 123, 153. Granting Stone access to these documents would allow him to invade the internal strategy of his political opponents—simply by issuing the subpoena to CrowdStrike as opposed to the DNC and DCCC—and would reveal highly sensitive and privileged materials that have no evidentiary value in his criminal proceedings, all while

² See Daniel R. Coats, *Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community*, Office of the Director of National Intelligence (Feb. 13, 2018) <https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf> at 6, (“We expect that Russia will conduct bolder and more disruptive cyber operations during the next year,” including “hack-and-leak influence operations.”).

leaving the DNC and DCCC with little opportunity to protect their interests.

Finally, in considering Stone's request, context matters. The indictment in this case alleges that Stone not only obstructed investigations into Russian interference in the 2016 presidential election, but also requested the release of stolen emails that he believed would be damaging to the Democratic presidential nominee. ECF 1 ¶ 30. He has already violated this Court's orders by posting repeatedly on social media about court proceedings, including, notably, several posts referencing the CrowdStrike reports. ECF 136 at 4-5. And now he seeks access to unredacted versions of the reports—which contain privileged and highly sensitive materials, created at the behest of the DNC's and DCCC's legal counsel in the aftermath of a *politically motivated* cyberattack that Stone allegedly attempted to exploit for political gain, ECF 1 ¶ 30—but provides no details on “what he expect[s] to find and why he expect[s] to find it.” *United States v. Bing Tang Vo*, 78 F. Supp. 3d 171, 181 (D.D.C. 2015). Such requests, particularly when directed toward a litigant's political opponents, require heightened vigilance to prevent the abuse of the subpoena process; and the concerns the DNC and DCCC have raised, in addition to Stone's failure to demonstrate any legitimate basis for seeking the unredacted reports, provide all the more reason why this Court should deny his request to subpoena CrowdStrike.

BACKGROUND

In the 2015-2016 election cycle, the DNC, DCCC, and other high-profile Democrats were victimized by an unprecedented, politically motivated cyberattack, which the intelligence community and law enforcement officials have universally concluded was orchestrated by Russian intelligence operatives.³ In the aftermath of the attack—once the DNC and DCCC learned of it—counsel for the DNC and DCCC retained CrowdStrike, a cybersecurity technology firm, to conduct a forensic analysis of the intrusion in order to assist counsel in advising both political organizations on issues related to the breach. Counsel for the DNC and DCCC subsequently provided redacted versions of these reports to law enforcement officials, protecting from disclosure highly sensitive,

³ See, e.g., Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf

privileged materials relating to remediation efforts and future strategic plans. ECF 123 at 1-3.

On January 24, 2019, a grand jury returned a seven-count indictment against Roger Stone (“Stone Indictment”) for obstructing the investigations into Russian interference in the 2016 presidential election (count 1); making false statements before the U.S. House of Representatives Permanent Select Committee on Intelligence (“HPSCI”) and U.S. Senate Select Committee on Intelligence (“SSCI”) (counts 2-6); and witness tampering (count 7). ECF 1. The indictment alleges that Stone made numerous false statements concerning his possession of documents pertinent to HPSCI’s investigation, *id.* ¶¶ 21-23; his contacts and communications with an entity referenced in the indictment as “Organization 1,” *id.* ¶¶ 25-34; his communications with the Trump campaign, *id.* ¶ 35; and that Stone attempted to prevent another witness from cooperating with the investigation, *id.* ¶¶ 36-39.

The CrowdStrike reports and the false statements alleged in the Stone Indictment are largely unrelated. The indictment makes passing reference to the DNC’s and DCCC’s retention of a “security company . . . to identify the extent of the intrusions” in its introductory explanation of the 2016 cyberattack but does not otherwise cite or rely upon the reports created as part and parcel of that company’s investigation in any of the allegations against Stone. *Id.* ¶ 1. Nonetheless, Stone has filed to date a motion to compel unredacted versions of the CrowdStrike reports, ECF 103, and a separate request to issue a Rule 17(c) subpoena to CrowdStrike for the unredacted reports along with all drafts. ECF 160.

In both motions, Stone makes no argument that the reports either refute or support the perjury or witness tampering allegations against him, nor does he identify any portion of the reports—which the Government provided in redacted form—that would suggest that the limited redactions contain information that is in any way relevant to these proceedings. Instead, Stone’s subpoena request seeks to turn his own criminal trial into a fishing expedition against his political opponents, who were the victims of a crime that Stone is alleged to have exploited for his own political ends.

ARGUMENT

A. The DNC and DCCC are Entitled to Assert Their Interests in Preventing the Disclosure of Privileged and Highly Sensitive Documents in These Proceedings.

At issue in this Motion is the threatened disclosure of highly sensitive and privileged materials that have been redacted from internal reports that were commissioned by counsel for the DNC and DCCC, and the release of which would cause significant harm to these political organizations. Although the Federal Rules of Criminal Procedure do not expressly provide for intervention, “[f]ederal courts have frequently permitted third parties to assert their interests in preventing disclosure of material sought in criminal proceedings or in preventing further access to materials already so disclosed.” *United States v. Hubbard*, 650 F.2d 293, 311 n.67 (D.C. Cir. 1980) (citing cases). The DNC’s and DCCC’s “interest in protecting privileged materials from compelled disclosure is threatened,” and the Government has made clear that it does not intend to enforce that interest, ECF 164, thus Stone’s request presents “a paradigmatic case of entitlement to intervention as of right.” *In re Grand Jury Proceedings*, 201 F. Supp. 2d 5, 9 (D.D.C. 1999).

While the proposed subpoena is directed to CrowdStrike, any potentially responsive records that CrowdStrike may have consist of attorney work product prepared for the DNC and DCCC; as such, the privileges implicated by the redacted portions of the CrowdStrike reports also belong to the DNC and DCCC. Neither the Government nor CrowdStrike are appropriately positioned to protect those interests,⁴ and thus intervention, for the limited purpose of challenging Stone’s subpoena request, is warranted. *See id.* (“[T]hough the grand jury subpoenas sought to be quashed are directed to the [] firm and not to [the movant] any asserted attorney-client privilege attaching to these documents would be held by the [client movant].”).

B. Stone’s Subpoena Request is Improper Because it Fails to Establish the Relevance of the Materials He Seeks.

At the outset, Stone’s Motion makes clear that he is engaged in a fishing expedition and

⁴ The Government, while noting that the CrowdStrike reports are not relevant to the charges against Stone, ECF 123 at 2-3, has indicated that it does not intend to file any response to Stone’s request to subpoena CrowdStrike, ECF 164.

cannot meet the Rule 17 requirements. *See* Fed. R. Crim. P. 17(c). It is well established that “[a] subpoena duces tecum may not be used for the purpose of discovery . . . to ascertain the existence of documentary evidence,” “[r]ather, it may be used to obtain only evidentiary materials,” and “[t]he burden rests with the party issuing a subpoena to show (1) relevancy; (2) admissibility; and (3) specificity.” *United States v. Binh Tang Vo*, 78 F. Supp. 3d 171, 180 (D.D.C. 2015) (citations and quotation marks omitted). “[M]aterials may be subpoenaed under Rule 17(c) only if there is a good-faith effort made to obtain evidence.” *United States v. Edwards*, 191 F. Supp. 2d 88, 89 (D.D.C. 2002) (quotation marks omitted). Stone’s request, in contrast, fails to demonstrate the relevance or admissibility of the materials he seeks from CrowdStrike, and his explanation of what he hopes to find in the unredacted reports is entirely vague. His Motion merely alleges that the unredacted copies “likely contain evidence that is material to the Defendant’s innocence,” but does not even attempt to explain what that evidence might be, ECF 160 at 1-2. He similarly concludes, without elucidating information or explanation, that the unredacted reports are necessary to prove the materiality provision of the perjury counts. *Id.*

Both claims defy logic when compared with the allegations in his indictment. Stone is alleged to have testified falsely concerning his possession of documents pertinent to HPSCI’s investigation, ECF 1 ¶¶ 21-23; his contacts and communications with an entity referenced in the indictment as “Organization 1,” *id.* ¶¶ 25-34; his communications with the Trump campaign, *id.* ¶ 35; and is also alleged to have attempted to prevent another witness from cooperating with the investigation, *id.* ¶¶ 36-39; but, as the Government has previously explained, he is not charged with conspiracy to hack the DNC or DCCC. ECF 123 at 2. The unredacted CrowdStrike reports do not have any clear connection to any of these charges against him, and Stone’s subpoena request does little to explain how any of these materials could possibly be relevant to his defense, other than to baldly speculate that they may exonerate him.

Rule 17(c) requires more: specifically, “[a] link that explains what the [movant] expected to find and why [he] expected to find it.” *Binh Tang Vo*, 78 F. Supp. 3d at 181. This “specificity requirement” is satisfied if “there is a substantial likelihood, demonstrated through rational

inferences, that the documents being sought contain relevant and admissible evidence.” *Id.* (quoting *United States v. Libby*, 432 F. Supp. 2d 26, 31 (D.C. Cir. 2006)). Stone’s subpoena request contains no such explanation and falls well short of the applicable Rule 17(c) standards, thus his Motion to Subpoena CrowdStrike should be denied on that basis alone.

C. Stone’s Subpoena Request Seeks to Invade the DNC’s and DCCC’s Attorney-Client, Attorney Work Product, and First Amendment Privileges.

Compounding Stone’s failure to establish the relevance of the documents he seeks is the inevitable intrusion on the attorney-client privilege, attorney-work product doctrine, and the First Amendment privileges held by the DNC and DCCC. As the Government explained in previous filings, CrowdStrike prepared the reports at the direction of the DNC’s and DCCC’s legal counsel, ECF 123 at 1, for the purpose of providing legal advice and in anticipation of possible legal action by or against the DNC or DCCC. “So long as obtaining or providing legal advice was one of the significant purposes of [an] internal investigation ... even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of the company discretion,” attorney-client privilege protects communications among a client, client’s counsel, and entities engaged to assist in the investigation. *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 758-59 (D.C. Cir. 2014).

The privilege, moreover, extends not just to communications that explicitly contain legal advice or opinion work product, but also covers “purely factual exchanges” in the context of an internal investigation conducted by non-attorneys, “when those facts are provided to the attorney at his request for the purpose of enabling him to provide legal advice.” *Fed. Trade Comm’n v. Boehringer Ingelheim Pharm., Inc.*, 180 F. Supp. 3d 1, 16 (D.D.C. 2016), *aff’d*, 892 F. 3d 1254 (D.C. Cir. 2018). The proposed subpoena attached to Stone’s Motion plainly intrudes on these privileges by seeking all unredacted drafts and final reports issued by CrowdStrike to counsel for the purpose of counsel providing legal advice relating to the DNC and DCCC cyberattack; accordingly, the reports are subject to the attorney-client privilege and the work product doctrine.

And because the DNC and DCCC are political organizations, Stone’s broad request for all

unredacted reports relating to a politically motivated cyberattack also threatens to intrude upon internal deliberations and strategy, the disclosure of which may cause significant First Amendment injury. Here, the application of the First Amendment privilege “turns not on the type of information sought, but on whether disclosure of the information will have a deterrent effect on the exercise of protected [First Amendment] activities.” *Perry v. Schwarzenegger*, 591 F.3d 1147, 1162 (9th Cir. 2010) (citing *Nat’l Ass’n for Advancement of Colored People v. State of Alabama ex rel Patterson*, 357 U.S. 449, 460-61 (1958)). Where the release of confidential, internal communications might “encourage[] political opponents” to harass their competitors with discovery requests “to serve the dual purpose of ‘chilling’ the expressive efforts of their competitor and learning their political strategy so that it can be exploited to the complainant’s advantage” or otherwise “frustrate [political parties’] decisions as to ‘how to organize’ [themselves], [or] conduct . . . [their] affairs,”” *Am. Fed’n of Labor & Cong. Of Indus. Organizations v. Fed. Election Comm’n*, 333 F.3d 168, 177-78 (D.C. Cir. 2003) (citing *Eu v. San Francisco Cty. Democratic Cent. Comm.*, 489 U.S. 214, 230-31 & n. 21 (1989)), the First Amendment protects such materials against compelled disclosure. *See id.*; *see also Ohio Organizing Collaborative v. Husted*, 2:15-cv-01802, 2015 WL 7008530, at *3 (S.D. Ohio Nov. 12, 2015) (rejecting argument that plaintiffs could only demonstrate First Amendment infringement if they presented evidence of threats, harassment, or reprisals, and recognizing the proper test is whether the party invoking the privilege “demonstrate[s] an objectively reasonable probability that” disclosure “would have a chilling effect on [their] First Amendment associational rights”).

Allowing a litigant to obtain materials reflecting a political opponent’s internal strategy, including materials that potentially jeopardize its cybersecurity, poses a serious risk of chilling First Amendment protected activity. In this case, it would hinder the DNC’s and DCCC’s ability to work with cybersecurity specialists to advance their missions and defend against politically motivated attacks like the one that occurred in the 2016 presidential election. *Id.* (“[D]isclosure of such sensitive information in the context of highly charged litigation involving issues of great political controversy would have a chilling effect on plaintiffs’ freedom of association by adversely

impacting their ability to organize, promote their message(s), and conduct their affairs.”). Compelled disclosure of the unredacted reports under these circumstances would set a troubling precedent and would incentivize parties to harass political entities like the DNC and DCCC through the discovery process.

CONCLUSION

For the reasons set forth above, the DNC and DCCC respectfully request that their Motion for Leave be granted and Defendant’s Motion to Subpoena CrowdStrike be denied.

Dated: August 8, 2019

Respectfully submitted,

/s/ Uzoma Nkwonta

Marc E. Elias

Uzoma N. Nkwonta

PERKINS COIE LLP

700 Thirteenth Street, N.W., Suite 600

Washington, D.C. 20005-3960

(202) 654-6200

(202) 654-6211 (fax)

MElias@perkinscoie.com

UNkwonta@perkinscoie.com

*Counsel for the Democratic National Committee
and DCCC*